



SUNBELT SOFTWARE

iHateSpam Server Edition™

for Microsoft Exchange 2000 Servers

User Guide

Use of this software is subject to the End User License Agreement found in this User Guide (the "License Agreement"). By installing the software, you agree to accept the terms of the License Agreement. Copyright (c) 2002 Sunbelt Software Distribution, Inc. All rights reserved. Sunbelt Software, the Sunbelt Logo, "Eliminate annoying spam", "The ultimate weapon against junk email", the robotic character and iHateSpam are trademarks of Sunbelt Software. All products mentioned are trademarks or registered trademarks of their respective companies.

CHAPTER 1: INTRODUCTION TO IHATESPAM SERVER EDITION	3
SYSTEM REQUIREMENTS.....	3
OVERVIEW OF SETUP	3
INSTALLING IHATESPAM SERVER EDITION.....	3
<i>Exchange 2000 Event Sink Setup.....</i>	<i>4</i>
<i>Spam Filtering Report Database Setup</i>	<i>4</i>
THE IHATESPAM PROGRAM DISPLAY	4
CHAPTER 2: SYSTEM MANAGEMENT.....	6
GENERAL SYSTEM SETTINGS	6
REPORTING SETTINGS	7
REGISTRATION.....	8
SMTP EVENTS MANAGEMENT	9
PUBLISHING SETTINGS	10
CHAPTER 3: SPAM FILTERING.....	11
GENERAL FILTERING SETTINGS	11
GLOBAL FILTERS	12
<i>Whitelisted and Blacklisted Senders.....</i>	<i>12</i>
<i>Blocked Character Sets.....</i>	<i>12</i>
<i>Custom Filtering Rules.....</i>	<i>13</i>
<i>Assigning Weights to Custom Rules.....</i>	<i>14</i>
<i>Filter Plug-Ins</i>	<i>15</i>
EXPORTING FILTER LISTS	16
POLICY SETTINGS	16
ASSIGNING USERS TO A POLICY.....	18
FILTER PIPELINE	20
CHAPTER 4: IHATESPAM REPORTS	21
USER REPORTS	21
<i>Messages Captured by User</i>	<i>21</i>
<i>Top 50 Users Receiving Spam</i>	<i>22</i>
SYSTEM REPORTS	23
<i>Number of Messages Captured.....</i>	<i>23</i>
<i>Spam vs. Non-spam.....</i>	<i>24</i>
<i>Messages Captured by Each Filter.....</i>	<i>25</i>
<i>Messages Handled by Filtering Engine.....</i>	<i>26</i>
CHAPTER 5: IHATESPAM TOOLS AND SUPPORT	28
REPORT DATABASE INSTALLATION UTILITY	28
SMTP EVENTS INSTALLATION UTILITY.....	28
ERROR LOGS.....	29
TECHNICAL SUPPORT.....	29
INDEX	30
END USER LICENSE AGREEMENT FOR IHATESPAM SERVER EDITION.....	31

Chapter 1: Introduction to iHateSpam Server Edition

iHateSpam Server Edition from Sunbelt Software is the solution to unsolicited email (or "spam") that fills up your company's servers, slows down your network, and lowers the productivity of your employees. With iHateSpam Server Edition, your employees can stop wasting valuable time sorting through junk email. Instead, spam is caught and deleted at the server level based on filtering criteria specified by the system administrator.

- ❑ iHateSpam Server Edition runs on a Windows 2000 Server in conjunction with Exchange 2000.
- ❑ iHateSpam Server Edition utilizes the Microsoft Management Console environment, which offers simplified administration through integration, delegation, task orientation, and overall interface simplification.
- ❑ iHateSpam Server Edition offers global filtering, which affects all users, and the ability to create "policies" which filter email for specific groups of individuals. In addition, it allows users to maintain their own whitelists, blacklists and quarantine folder.
- ❑ To facilitate administration, iHateSpam Server Edition includes a collection of reporting, and scheduling tools.

System Requirements

iHateSpam Server Edition requires the following combination of hardware and software for optimal performance:

- ❑ Windows 2000 Server with Service Pack 2 or later.
- ❑ MS Exchange 2000 with Service Pack 2 or later.
- ❑ MSSQL 2000 or MSDE 2000 for reporting.
- ❑ Pentium II 500mhz processor with 256 megs RAM (minimum), Pentium III 1000 with 512 megs RAM (recommended).

Overview of Setup

Filtering your incoming email with iHateSpam Server Edition involves the following steps, all of which are accomplished via wizard screens and straightforward dialogs:

1. Installing the software on your Windows 2000 server. (See below.)
2. Configuring a few system settings under "System Management". (See Chapter 2.)
3. Configuring a few general filtering settings under "Spam Filtering".
4. Setting up global filters that govern all of your email users.
5. Creating policies (collections of filtering criteria) that affect specific groups of users.
6. Adding specific users to your policies. (For steps 3 through 6, see Chapter 3.)

Installing iHateSpam Server Edition

The iHateSpam Server Edition installation program consists of a series of easy to follow wizard screens. When installing iHateSpam, you should be aware of the following configuration issues.

Exchange 2000 Event Sink Setup

iHateSpam Server Edition connects to your Exchange 2000 SMTP Server Gateway via SMTP OnArrival Event Sinks. The SMTP OnArrival Event Sink must be registered with iHateSpam in order to provide email filtering capabilities to your email users. You must install an SMTP Event Sink on each of your Exchange SMTP services as well as all instances of the services that Exchange uses. For more information about SMTP Event Sinks, see Chapter 2: Configuring iHateSpam ("SMTP Events Management") and *Chapter 5: iHateSpam Diagnostic Tools and Support* ("SMTP Events Installation Utility").

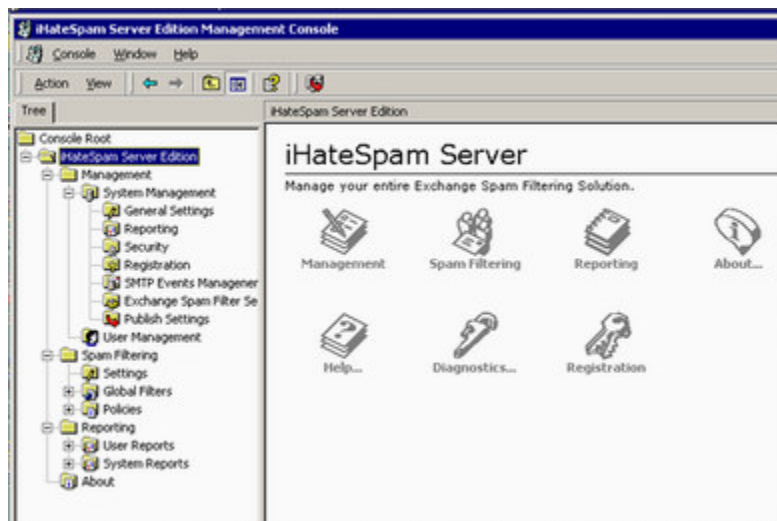
Spam Filtering Report Database Setup

The report generating component can be installed when you install the iHateSpam filtering engine on your Exchange server. You can also install it later by running the Report Database Installation Utility from the Tools menu [Start/Programs/iHateSpam/Tools]. If you opt to install the reporting component during installation, you are asked to provide information on how to connect to your SQL database server.

The iHateSpam Program Display



iHateSpam uses Microsoft's Management Console, with its Windows Explorer-like design, as its user interface.






Folders containing program options are listed in a tree display in the left pane. When an option is highlighted on the left, its customization screen appears in the large right-hand pane.



iHateSpam Server Edition Display

Different options appear on the iHateSpam toolbar depending on the task you are performing. At various times, the following icons appear on the toolbar.

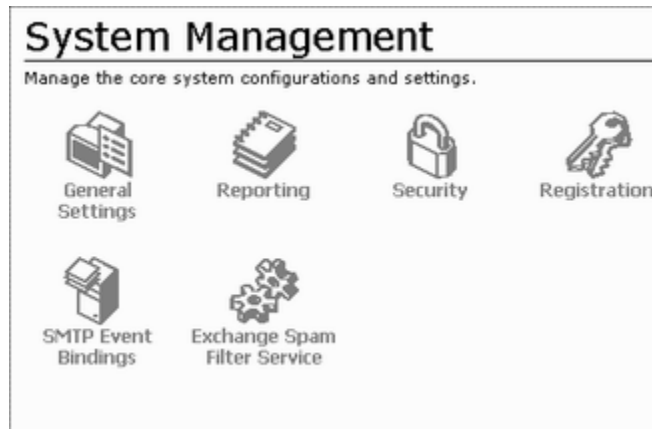
	Register the program using a valid Registration Key.
	Add a new address to a whitelist or blacklist.

	Block emails consisting of foreign characters.
	Create a new custom rule for filtering email.
	Add a filter plug-in to your configuration.
	Create a new policy of filtering criteria.
	Export a list of filtering criteria to a text file.

Chapter 2: System Management

After installing iHateSpam Server Edition on your Exchange 2000 server, it is important to verify that your system management settings are configured according to your circumstances and preferences. This will ensure that your users' email is optimally filtered.

The **System Management** folder is located within the Management folder in the left pane of the Management Console. Highlight any category in the System Management folder to display its options in the right pane.



Options in the System Management folder.

General System Settings

System Activation

Allows you to enable or disable filtering on a system-wide basis.

NOTE: To completely disable filtering, it is recommended that you delete all event sink bindings rather than setting System Activation to Off. For further information, see SMTP Events Management.

Logging Mode

Specifies the method (**File** or **Event Log**) to be used for recording information about the tasks performed by iHateSpam Server Edition. This information can be useful in diagnosing problems that occur during filtering. We recommend that you set this option to **File**, as this option produces a much smaller log file containing iHateSpam-specific information.

System Management: General Settings

Select your general system settings below and press the Update button to have these settings take place. Please note, that settings in the system are not stored until you publish these settings to refresh the in memory database of the service. Please refer to the help file for further details.

[Help](#)

System Activation: Turn the entire spam filtering on or off. ?
☒ On ☐ Off

Logging Mode: Set the logging mode of the system.
 Logging is used to record possible system errors or anomalies that can be used to diagnose any issues that can be occurring.
☒ File (recommended) ☐ Event Log

Trace Mode: Turn system tracing on or off.
 Tracing is used to record all events in the system to various trace files. This option should only be used if recommended by support as it can produce very large log files on the system as well as decreases the system's overall performance on spam filtering.
☐ On ☒ Off

Update

Note: All updates are saved to the local cache. For updates to populate to the service, you must publish your update. Your local cache is automatically saved until you publish it.

General Settings (System Management)

Trace Mode

Allows you to record all events that occur during email filtering and store the information in various "trace" files. Tracing creates very large log files and can negatively impact the system's overall performance. Therefore, it should only be used during troubleshooting at the direction of technical support personnel.

After making changes to these settings, click **Update** to save them to your local XML configuration files. Updates are populated to the system within 5 minutes using the Smart Cache feature or can be forced by using the Clear Smart Cache option.

Reporting Settings

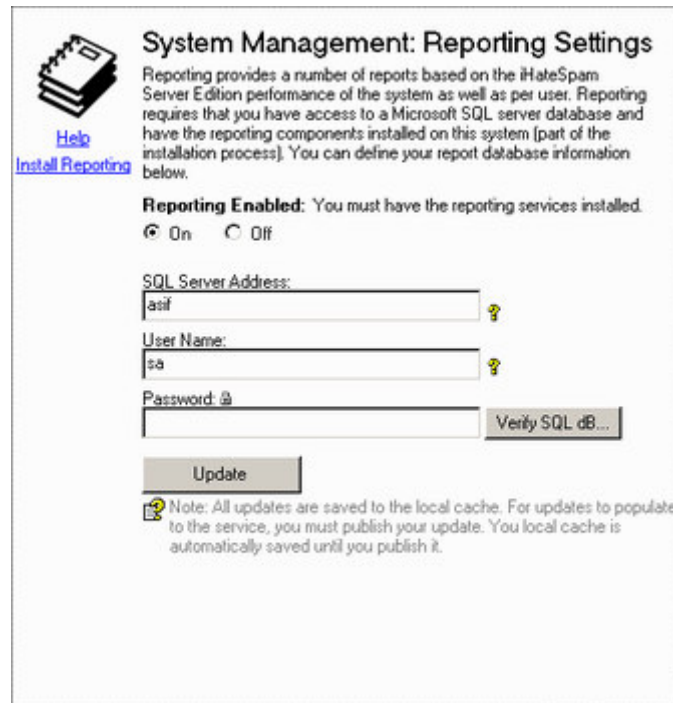
If you opted to install the reporting component during the initial installation of iHateSpam Server Edition, the report database "SpamMetabase" will have been installed on your SQL server. On the Reporting Settings screen you enable report and provide access information for the SQL server. Note that currently only MSSQL 2000 and MSDE 2000 are supported for reporting.

Reporting Enabled

If you installed the reporting option during installation, you can turn on reporting here.

SQL Server Address

Enter the server IP address or computer name of your SQL server here.



System Management: Reporting Settings

Reporting provides a number of reports based on the iHateSpam Server Edition performance of the system as well as per user. Reporting requires that you have access to a Microsoft SQL server database and have the reporting components installed on this system (part of the installation process). You can define your report database information below.

Reporting Enabled: You must have the reporting services installed.
☒ On ☐ Off

SQL Server Address: ?

User Name: ?

Password:

Note: All updates are saved to the local cache. For updates to populate to the service, you must publish your update. Your local cache is automatically saved until you publish it.

Reporting Settings (System Management)

User Name and Password

Enter the username and password you use to access your SQL database here. *SQL authentication must be used.*

When you are done, click **Verify SQL Database** to verify that the information you entered on this screen is correct and then click **Update** to save them to your local cache. Updates are populated to the system within five minutes using the Smart Cache feature or can be forced by using the Clear Smart Cache option.

Registration

Sunbelt Software offers a fully functional, 30 day demonstration version of iHateSpam Server Edition. If you choose not to register the software, the demo version expires at the end of the 30 day trial period. Once the software expires, spam filtering no longer takes place and messages are routed as normal.

To continue using iHateSpam Server Edition, you must obtain a valid Registration Key from Sunbelt Software. The key allows you to filter the email messages of a specific number of Exchange users. (The license for each user is referred to as a "seat".)

IMPORTANT NOTE: *In the event your software expires, you will not have to reinstall or reconfigure the software once you obtain a valid Registration Key. Simply enter your key (as described below) and the system continues filtering email as if it had not been interrupted.*



Registration

In order to run the iHateSpam Server Edition for Exchange you need to register this product after the demo period expires. After the demo has completed, all spam filtering will no longer function and messages will be routed as normal.

[Help](#)

Registration Key: Use this key to unlock the full product. If you have purchased a registration key for iHateSpam Server Edition, please enter the key below. In addition, you must enter the number of seats you have purchased as well.

Registration Key:

Number of Seats: 

iHateSpam Registration Screen

To register the software:

1. Display the Registration screen by selecting **Registration** (under System Management) in the left pane **OR** by clicking the **Registration icon** on the toolbar.
2. Enter the **registration key** you obtained from Sunbelt Software.
3. Enter the **number of seats** covered by the registration key.
4. Click **Update Registration**.
5. Clear the Smart Cache using the button under System Management/Smart Caching.

SMTP Events Management

iHateSpam Server Edition connects to your **Exchange 2000 SMTP Server Gateway** via **SMTP OnArrival Event Sinks**. The SMTP OnArrival Event Sink must be registered with iHateSpam in order to provide email filtering capabilities to your email users. You must install an SMTP Event Sink on each of your Exchange SMTP services as well as all instances of the services that Exchange uses.

You can install SMTP event sinks through the Management Console by selecting **SMTP Events Management** (under System Management) **OR** by running the **SMTP Events Installation Utility** from the **Tools** menu (**Start/Programs/iHateSpam/Tools**).



Installing Event Sink Bindings

If one or more SMTP instances are listed as requiring installation of an Event Sink, place a check in the appropriate checkbox. If all SMTP instances have Event Sinks installed, existing instances are grayed out and cannot be checked. In addition, a message is displayed indicating that all SMTP Instances have Event Sinks installed.

Also displayed on this screen are **Current Service Statistics**. You can refresh the display and update the statistics by clicking the **refresh icon** next to Current Service Statistics.

Publishing Settings

Changes to your iHateSpam Server Edition settings are stored and published using iHateSpam Server Edition's **Smart Cache feature**. When you make changes to your settings, they do not go into effect immediately. Rather, they are saved to the program's configuration files which are composed of 2 XML documents in the installation directory. By default, the configuration file is scanned for changes every five minutes.

You can also force the changes to be picked up immediately on the local server by selecting **Smart Cache** (under System Management) in the left pane and selecting the **Clear Cache** button.

To copy the configuration file to additional Exchange servers running iHateSpam Server Edition, select **Replication** (under System Management) from the left pane. The updated file is detected by the remote machine within five minutes and the new settings loaded.

Once the above settings are properly configured, you will define the criteria for filtering your incoming email and apply those rules to your users, as described in the next chapter.

Chapter 3: Spam Filtering

In order for iHateSpam Server Edition to filter your incoming email according to your specifications, you must:

- ❑ Configure a few general filtering settings.
- ❑ Define the global filters that govern filtering for all users.
- ❑ Create "policies" (collections of filters that apply to specific groups of users).
- ❑ Add users to the policy that is appropriate for their situation.

The steps involved in these tasks are described in this chapter and are performed by selecting the appropriate option (General Settings, Global Filters, or Policies) from the Spam Filtering folder.



General Filtering Settings

Disable Bounce Message Filtering

If this option is **enabled**, bounced messages generated by the email server MAILER-DAEMON or POSTMASTER are not filtered. Rather, they are routed normally by the Exchange service. If this option is **disabled**, such bounced messages are treated as normal external email messages and filtered based on the policy rules in effect for that addressee.



General Spam Filter Settings

Spam Definitions

iHateSpam Server Edition uses Sunbelt Software's proprietary "**spam definitions**" to determine which email messages are legitimate and which are unwanted email. Sunbelt is

constantly updating its spam definitions in order to provide its users with the most accurate email filtering possible. It is important that you update your spam definitions regularly in order to ensure optimal performance.

To update your definitions:

Make sure that your system has Internet access and allows traffic via port 80 (HTTP) and then click the **Update Definitions** button.

Global Filters

Global Filters are spam filtering rules that **govern all users** within the email system (as opposed to policies, which are collections of rules that apply to specific groups of users). The spam filter types described below can be applied globally or to a policy, depending on whether the changes are made from within the Global Filter folder or a Policy folder. (All of these options are contained within the Global Filter and each Policy folder that exists on the server.)

Whitelisted and Blacklisted Senders

Whitelist Rules specify email addresses, domains, or names that should **always** be delivered to the mailbox of the recipient. **Blacklist Rules**, on the other hand, specify email addresses, domains, or names that are **never** allowed to be delivered to the mailbox of the recipient. Instead, they are either deleted or sent to the user's quarantine folder depending upon the policy option "Delte."



To add an address to a whitelist or blacklist:

1. Select **Whitelist** or **Blacklist** from the Global Filters folder (if the filter should apply to all users) **OR** from the appropriate Policies folder (if the filter applies to a policy).
2. Click the **Add New Address** icon on the toolbar.
3. Select the appropriate **Address Type** from the drop-down list.
4. Enter the **address, domain, or display name** you want to prevent from being filtered.
5. Click **OK**.

To delete an entry from a Whitelist or Blacklist:

1. Right-click on the entry you want to delete.
2. Select **Remove Whitelist Address** or **Remove Blacklist Address** from the context menu that appears. (A verification dialog appears.)
3. Click **OK** to remove the entry from the list or **Cancel** to cancel the request and leave the entry in the list.

Blocked Character Sets

A substantial percentage of junk email originates in foreign countries and is written using foreign character sets that cannot normally be displayed correctly on computers running the English version of Microsoft Windows. On this screen you can tell iHateSpam to filter all email messages written in one or more foreign character sets.

1. Select **Blocked Character Sets** from the Global Filter folder **OR** from a Policy folder to display a list of character sets that are being filtered for all users in the system **OR** those users assigned to the chosen policy, respectively.



To block a single character set:

1. Click the **Add New Blocked Character Set** icon on the toolbar.
2. Place a check next to the character set you want to block.
OR
Enter the name of a custom character set in the appropriate field and click **Add**.
3. Click **OK**.

To block all foreign character sets:

1. Right-click on the **Blocked Character List** (even if it is empty) to display the **Manage Blocked Character Set** dialog.
2. Place a check in the **Block All Non-ASCII-based Emails** (foreign character emails) checkbox.
3. Click **OK**.

***NOTE:** This option blocks all email written in any foreign character set that is not installed on the Exchange SMTP server for the user's account. When this option is applied globally, it overrides the settings in all policy filters.*

To delete a character set from the list:

1. Right-click on the entry you want to delete.
2. Select **Remove Character Set** from the context menu that appears. (A verification dialog appears.)
3. Click **OK** to remove the entry from the list or **Cancel** to cancel the request and leave the entry in the list.

Custom Filtering Rules

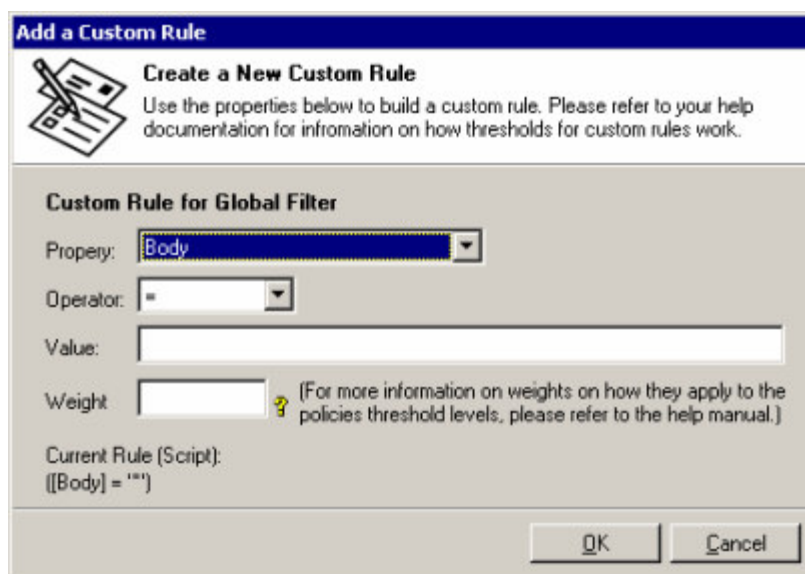
Custom rules are spam definitions created by the end user (as opposed to spam definitions created and continually updated by Sunbelt Software) and are based on message content. If an incoming message matches the criteria specified in the rule, the "weight" assigned to the rule is added to the message. Depending on the message's final weight (after all filters are applied), it will be deleted, quarantined, or forwarded to the recipient's mailbox. (For more information about weights, see "Assigning Weights to Custom Rules" below.)



To create a custom rule:

1. Click the **Add New Custom Rule** icon on the toolbar.
2. Select the **"property"** (such as "Subject") on which the rule is based using the drop-down menu.
3. Specify the **"operator"** (whether the above property should be identical to (=) or similar to (like) the value you will enter in the Value field).
4. Enter the **"value"** (what the property must be identical to or similar to in order for the message to be filtered).
5. Assign a **weight** to this rule.
6. Click **OK**.

***Example:** If the Property is Subject, the Operator is = (identical to), the Value is "Get Rich", and the weight is 500, then any email message with the subject "Get Rich" is assigned 500 points.*



Create a New Custom Rule Dialog

To modify an existing custom rule:

1. Right-click the rule you want to modify and select **Properties** from the context menu that appears.
2. Make the desired changes to the rule, then click **OK**.

To delete an entry from your list of custom rules:

1. Right-click on the entry you want to delete.
2. Select **Remove Custom Rule** from the context menu that appears. (A verification dialog appears.)
3. Click **OK** to remove the entry from the list or **Cancel** to cancel the request and leave the entry in the list.

Assigning Weights to Custom Rules

iHateSpam Server Edition uses a weighted points system to determine if an incoming email message is spam.

- ❑ Points are assigned to each rule used to screen incoming email. The number assigned can be positive or negative. (See the "Create a New Custom Rule" graphic above.)
- ❑ When a message meets the criteria of one or more rules, the points assigned to each filter are added to the message.
- ❑ When all rules have been applied to the message, the final number of points accumulated determines whether it is deleted, quarantined, or forwarded to the recipient's mailbox.

The Policy Settings screen of each policy allow you to specify "threshold" levels (the number of points that a message must accumulate before an action is taken).

Quarantine Threshold

Messages accumulating this number of points are sent to the user's Quarantine folder. The default threshold is 100. Setting this number below 60 may result in excessive false positives.

Delete Threshold

Messages accumulating this number of points are deleted from the mail server. The default threshold is 6000. At this setting no email will ever be deleted. Setting this value around 500-600 is safe for most organizations that want to have some spam deleted. Setting this value any lower than 200 is not recommended.

No Action Threshold

Messages accumulating this number of points are forwarded to the recipient's mailbox without further scanning. The default threshold is -1000.

If the default levels result in too much spam being allowed to reach your users' mailboxes or too many "false positives" (legitimate email being quarantined), you can adjust these levels.

Filter Plug-Ins

iHateSpam Server Edition allows the user of custom filter plug-ins to enhance the process of automatically eliminating unwanted email. A number of filter plug-ins are provided with the software and a developer SDK is also available for creating custom filters.

[Filter plug-ins are COM Objects and can be written in any programming language that can run as a COM object (such as C++ or Visual Basic). The COM Object must conform to the interface specified in the SDK. For detailed technical information regarding the creation of custom filter plug-ins, see the documentation that accompanies the SDK.]



To add a new custom filter to your global filters:

1. Select **Filter Plug-ins** from Global Filters in the left pane.
2. Click the **Add New Advanced Filter** icon on the toolbar to display the **Create a New Filter Plug-in** dialog.
3. Enter a **name** for this filter in the **Display Name** field.
4. Enter the plug-in's **ProgID** (object name and class).
5. Select the **Interface Type** to which the COM object was properly coded.
6. If the filter plug-in uses an **executable file (.EXE)** to manage its properties, use the **Browse** button to navigate to and select it.
7. Specify the **action to be taken** if the condition specified by the filter is met:
 - No Action** - No action is applied to the message.
 - Delete** - The message is removed from the server.
 - Quarantine** - The message is sent to the mailbox quarantine folder.
 - Add Weight** - The number of points entered in the Weight field are added or subtracted from the total filtering weight assigned to the message.
8. If you want the system to **stop processing filters** if this filter's condition is met, place a check in the **Stop Processing** checkbox.
9. Click **OK** to save your newly created plug-in.

Add An Filter Plugin

Create a New Filter Plugin
Select the Properties below to add an Filter Plugin. You need to know the ProgID of the COM Object that is to be used as the filter.

Filter Plugin for Global Filter

Display Name:

Application Details:

Prog ID: ?

Interface: ?

Properties: ?

Action:

Action: ?

☐ Stop Processing ?


Adding a Filter Plug-in to iHateSpam.

To import an existing custom filter to your global filters:

1. Follow steps 1 and 2 above, then click the **Import a Filter Plug-in** button.
2. Navigate to and select the plug-in you want to add to the policy and click **Open**.
3. Click **OK** to import the filter.

Exporting Filter Lists

Global or policy filter lists can be exported to text files as follows:

1. Display the list you want to export (for instance, global whitelist senders).
2. Click the **Export icon**  on the toolbar.
3. From the **Save As** dialog that appears, select a **location**, specify a **filename**, and select one of the following **file types** from the drop-down list:
Text (Tab Delimited *.txt)
Text (Comma Delimited *.csv)
Unicode Text (Tab Delimited *.txt)
Unicode Text (Comma Delimited *.csv)
4. Click **Save** to export and save the filter list.

Policy Settings

The Policy Settings screen allows you to define the rules for your default filtering policy (which specifies how email is to be filtered for all users who have not been assigned a specific policy) as well as any other policies you create.

PolicyID

Assigned automatically by iHateSpam.

Policy Name

When you create a new policy, iHateSpam assigns it a generic name such as "Policy 2".

Highlight this name and enter a more descriptive name in its place. (Do not change the name of the Default Policy.)

Enable Policy

Place a check in the Enable Policy checkbox to filter messages based on the rules set by this policy. (If desired, you can disable filtering for any user on the User Manager screen.)

Policy Settings

Policy Settings: (Default Policy) Default

Manage the setting for this policy in the sections below. Press the Update button after you have completed your modifications.

[Help](#)

Policy Details: Manage basic policy information.

Policy ID: 1 (This is the default policy, all unassigned users will have this policy.)

Policy Name: Default Policy

☒ Enabled policy. ?

Policy Thresholds

Quarantine Threshold:	200	? Default Threshold: 200
Delete Threshold:	1000	? Default Threshold: 1000
No Action Threshold:	-1000	? Default Threshold: -1000

Default Policy Settings (upper dialog)

Policy Thresholds

iHateSpam uses a weighted points system to determine whether or not incoming email is spam. The "weight" of a message is calculated across the various types of filters, which allows each filter to increase or decrease the cumulative "score" assigned to the message. In this section you specify the following:

Quarantine Threshold - The score that means "always quarantine".

Delete Threshold - The score that means "always delete".

No Action Threshold - The score that means "take no action".

Policy Exchange Folder Structures

Quarantine Folder Path: Spam/Spam - Quarantine/ ?

Whitelist Folder Path: Spam/Spam - Whitelist/ ?

Blacklist Folder Path: Spam/Spam - Blacklist/ ?

☒ Auto create whitelist folder ☒ Auto create blacklist folder ?

Policy Quarantine Actions

☐ Automatically delete messages that are in the blacklist ?

☒ Add X-Header to the message header

Append Subject Text: SPAM - ?

Update

? Note: All updates are saved to the local cache. For updates to populate to the service, you must publish your update. Your local cache is automatically saved until you publish it.

Default Policy Settings (lower dialog)

Policy Exchange Folder Structures

Folder Paths

Specify the Quarantine, Whitelist, and Blacklist folders to be created in the user's Exchange mailbox to hold whitelists, blacklists, and quarantined messages. When specifying the path, you must end with a trailing slash ("/").

Auto create whitelist/blacklist folder

If these options are checked (which is recommended), these folders are automatically created in the user's Exchange mailbox the first time email is processed for that user if they do not already exist.

Policy Quarantine Actions

In this section you specify actions to be taken when email is determined to be spam and quarantined.

Automatically delete messages in blacklist

If you check this option, messages from any sender in the user's blacklist folder or the global or group policy blacklist are automatically deleted.

Add X-Header to the message header

If you check this option an X-Header is appended to all quarantined messages. This header will also contain the message weight that was assigned to that message.

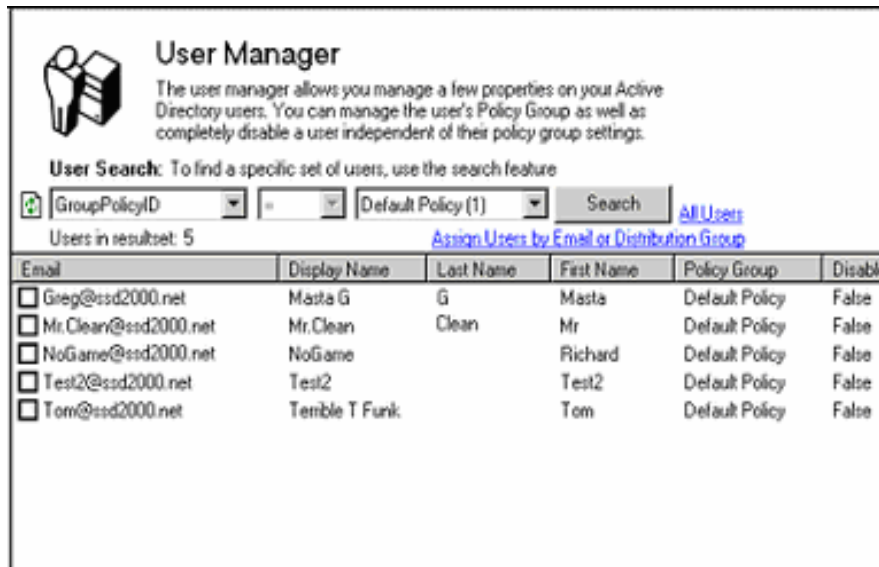
Append Subject Text

This is a field that is inserted at the beginning of the subject of the message, making the message quickly and easily identifiable to the user as spam.

After making changes to these settings, click **Update** to save them to your local cache. Updates are populated to the system within five minutes using the Smart Cache feature or can be forced by using the Clear Smart Cache option.

Assigning Users to a Policy

You assign users to a policy using the **User Manager** screen. User Manager is displayed when you select **User Management** (from within the Management folder in the left pane of the Management Console) **OR** by selecting **Assigned Users** from any Policy folder.



Assigning Users to a Policy with the User Manager screen.

Displaying a List of Users:

1. To display a list of all Active Directory users, click the **All Users** link.
You can refresh the list by clicking the **Refresh** icon to the left of the User Search fields.
2. To display a **subset** of the Active Directory user list, enter the appropriate search criteria in the User Search fields and click **Search**.

Managing Individual Users Assigned to a Policy:

1. Double-click an entry in the list (or right-click the entry and select **Edit User Properties**.) The **Manage User Properties** dialog displays.
2. Use the drop-down list to select the Policy Group you want to assign the user to OR enable/disable the user's spam filtering by clicking in the **Disable Filtering** checkbox, then click **OK** to save your changes.

Managing Multiple Users Assigned to a Policy:

1. Place a check next to the users you want to manage, then right-click.
2. From the menu that appears, select the action you want to perform.

Assign all checked users - Assign these users to this policy.

Enable all checked users - Enable this policy for these users.

Disable all checked users - Disable this policy for these users.

Adding Additional Users to a Policy:

1. Click the **Assign Users by Email or Distribution Group** link to display the **Assign Users to Policy** dialog. (This option is not available from within the User Management folder.)
2. To add one or more users to the policy by **Email Address** (the default search criteria), enter the user's email address in the Email Address field and then click **Add User**. The

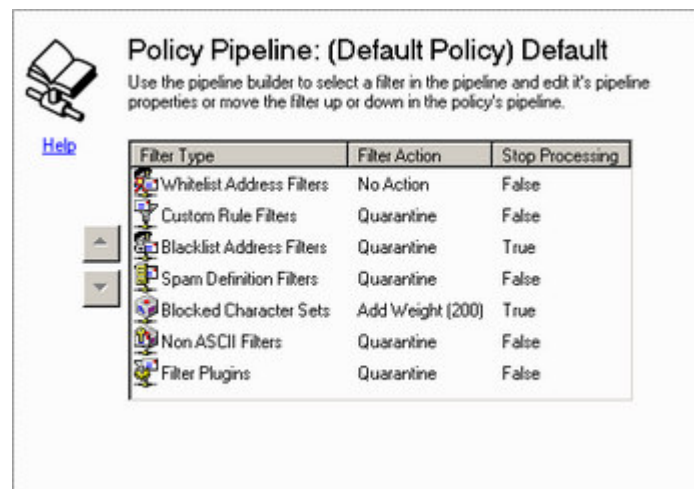
- name is added to the list below. (If the address you entered is not a valid email address, you will see a message to this effect.)
3. To add users by **Distribution Group**, click the Distribution Group link to change the search criteria, then select the desired group from the drop-down list. (The users who belong to that list are added to the list below.)
 4. When you are done, click **OK** to save your changes.

Filter Pipeline

The filtering criteria that make up a policy can be configured to create a customized filtering process for each user. Policy filters can be arranged in a specific order ("moved up and down the pipeline"). You can also specify the action to take when email meets the criteria specified by a filter (delete, quarantine, or no action).

To edit a policy's pipeline:

1. Double-click the **policy folder** in the left pane to display its contents.
2. Highlight **Filter Pipeline**. (The Policy Pipeline screen displays in the right pane.)
3. On the Policy Pipeline screen, highlight a **filter type** and make the desired changes to its properties. (Select the action you want to take based on the filter AND specify whether processing of that message should stop after this filter is applied. In some cases, you are also asked to assign a **weight** to the filter.)
4. If desired, use the **Up** and **Down** arrows to the left of the list to move the filter type up or down in the list. (Position of the filter may affect the outcome of the filtering process.)
5. When you are done making changes to the filter pipeline, click **Update** to save them to your local cache. Updates are not populated to the system until they are. Updates are populated to the system within two minutes using the Smart Cache feature. .



Policy Pipeline for the Default Policy

Chapter 4: iHateSpam Reports

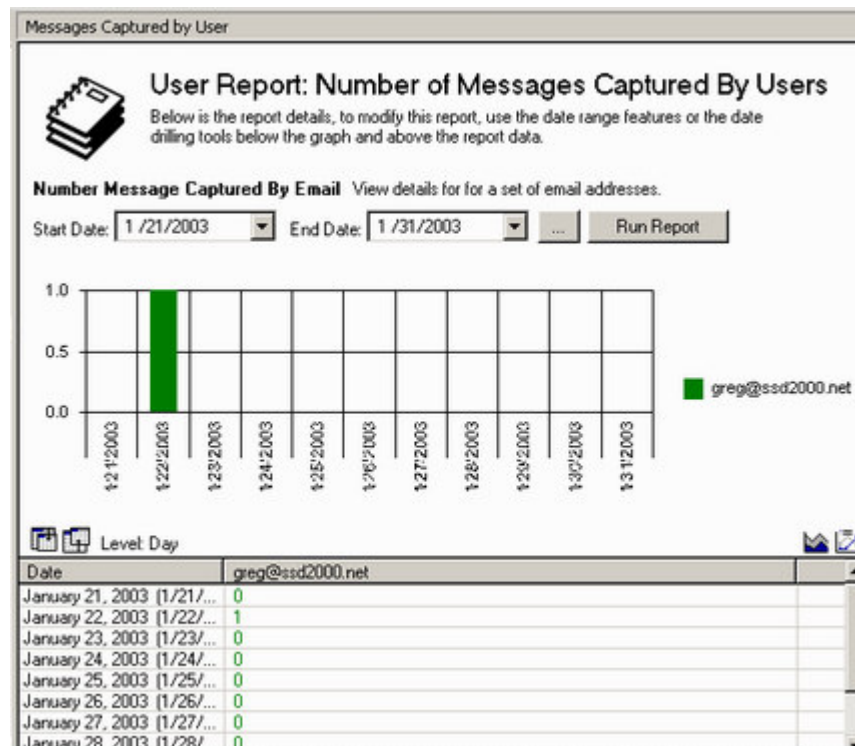
To assist you in evaluating the effectiveness of iHateSpam's email filtering and adjusting your filters and threshold levels to optimize performance, iHateSpam includes a reporting component. If this component is installed on your server, you can generate statistical reports for individual users as well as the system as a whole. Each report is displayed in both graphical and text format.

User Reports

The following User Reports are available.

Messages Captured by User

The "Messages Captured by User" report provides information on the amount of spam captured by the system that is addressed to one or more users during a configurable period of time.



User Report: Messages Captured by Users

To generate this report:

1. Select **Reporting** in the left pane to display the two categories of reports (**User Reports** and **System Reports**) in the right pane.
2. Click **User Reports** to display the different types of user reports available.
3. Click **Messages Captured by Email**.
(The **Filter Report by Email Address** dialog appears.)
4. Check the user (or users) you want to include in the report.
(If you do not know the user's email address, enter his or her last name in the **Last Name** field and click **Search**.)

- When the User Report is generated, you can narrow the scope of the report by selecting a **Start Date** and **End Date** and then clicking **Run Report**.

Once a report is generated, you can change it by selecting the following icons:



Browse button

Specify the email user you want generate a report on.



Roll Up Date and Roll Down Date

Click the appropriate icon to change the reporting period from **Day** to **Month** to **Year**.



Stack Chart and Unstack Chart

Display the bar graph with items/users "stacked" on top of each other (Stack) or placed next to each other (Unstack).

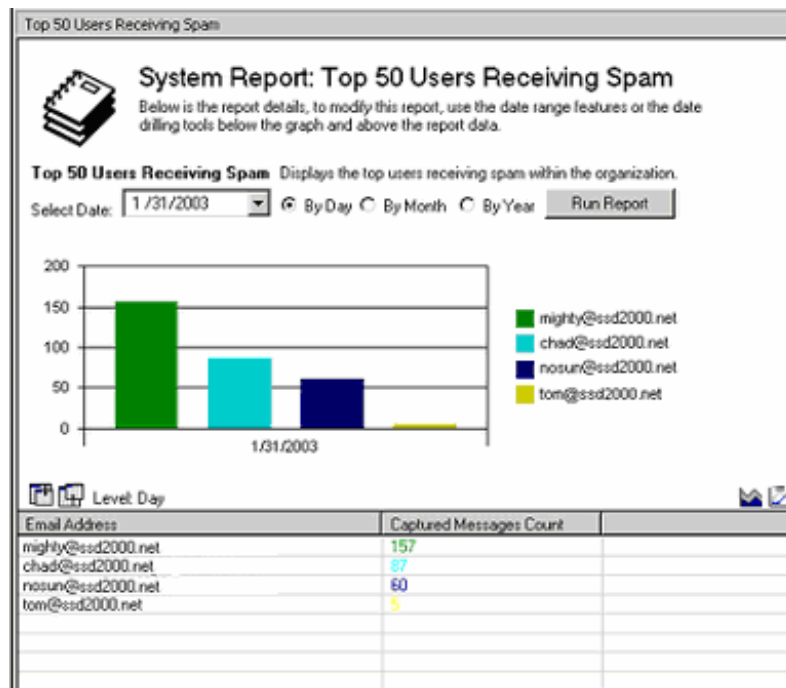


Show Chart Legend and Hide Chart Legend

Toggle the explanation of colors used to identify items/users.

Top 50 Users Receiving Spam

The "Top 50 Users Receiving Spam" report provides this information for a specific period of time.



User Report: Top 50 Users Receiving Spam

To generate a report:

- Select **Reporting** in the left pane to display the two categories of reports (**User Reports** and **System Reports**) in the right pane.
- Click **User Reports** to display the different types of user reports available.
- Click **Top 50 Users Receiving Spam**.

- When the Report is displayed, narrow or widen the scope of the report by selecting the period of time you want the report to cover (**By Day, By Month, or By Year**).
- Click **Run Report** to generate the new report.

Once a report is generated, you can change it by selecting the following icons:



Roll Up Date and Roll Down Date

Click the appropriate icon to change the reporting period from **Day** to **Month** to **Year**.



Stack Chart and Unstack Chart

Display the bar graph with items/users "stacked" on top of each other (Stack) or placed next to each other (Unstack).



Show Chart Legend and Hide Chart Legend

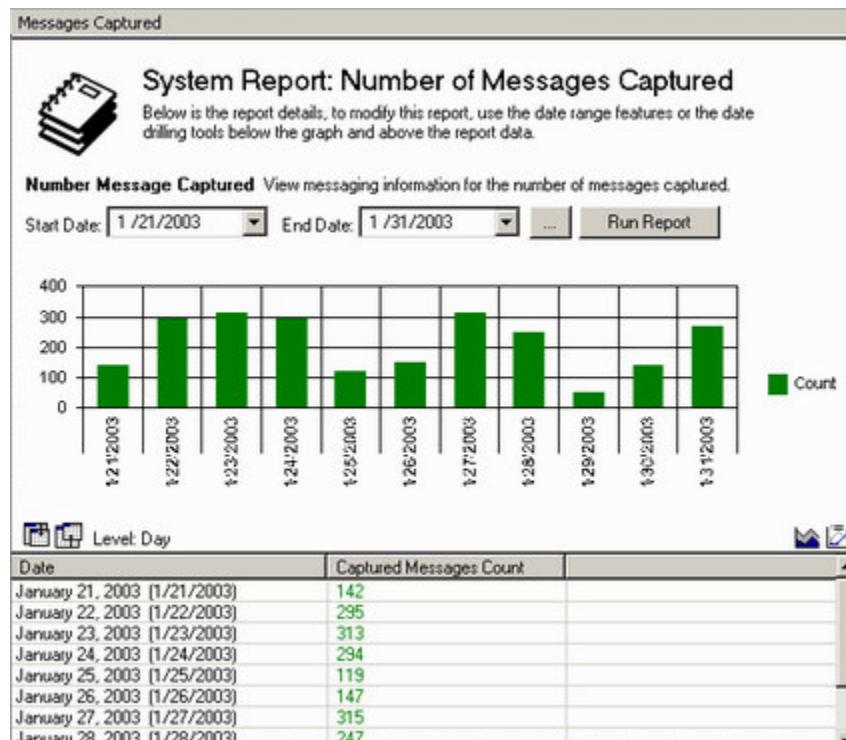
Toggle the explanation of colors used to identify items/users.

System Reports

The following System Reports are available.

Number of Messages Captured

The **Number of Messages Captured** report provides information regarding the amount of spam captured across the system during a user-specified period of time.



System Report: Number of Messages Captured

To generate a report:

- Select **Reporting** in the left pane to display the two categories of reports (**User Reports** and **System Reports**) in the right pane.
- Click **System Reports** to display the different types of system reports available.

3. Click **Number of Messages Captured**.
4. When the Report is displayed, narrow or widen the scope of the report by selecting a **Start Date** and **End Date**.
5. Click **Run Report** to generate the new report.

Once a report is generated, you can change it by selecting the following icons:



Browse button

Specify the email user you want generate a report on.



Roll Up Date and Roll Down Date

Click the appropriate icon to change the reporting period from **Day** to **Month** to **Year**.



Stack Chart and Unstack Chart

Display the bar graph with items/users "stacked" on top of each other (Stack) or placed next to each other (Unstack).

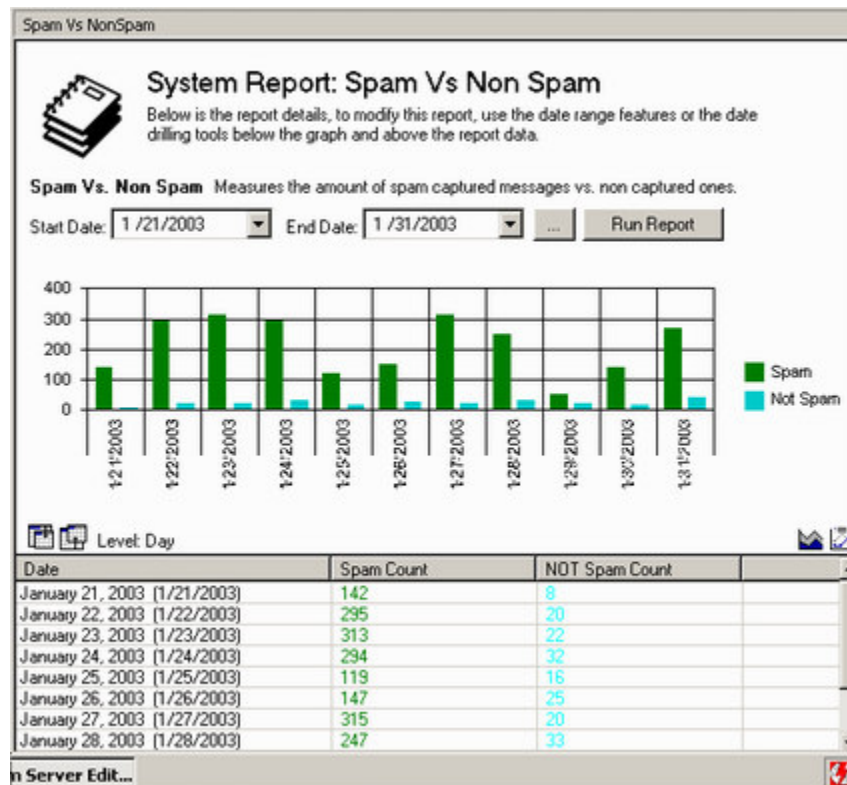


Show Chart Legend and Hide Chart Legend

Toggle the explanation of colors used to identify items/users.

Spam vs. Non-spam

The **Spam vs. Non-spam** report provides information regarding the amount of spam captured by the system during a user-specified period of time versus the amount of non-spam received during the same period.



System Report: Spam Vs. Non-Spam

To generate a report:

1. Select **Reporting** in the left pane to display the two categories of reports (**User Reports** and **System Reports**) in the right pane.
2. Click **System Reports** to display the different types of system reports available.
3. Click **Spam vs. Non-Spam**.
4. When the Report is displayed, narrow or widen the scope of the report by selecting a **Start Date** and **End Date**.
5. Click **Run Report** to generate the new report.
(Spam is shown in one color and legitimate email in another.)

Once a report is generated, you can change it by selecting the following icons:



Browse button

Specify the email user you want generate a report on.



Roll Up Date and Roll Down Date

Click the appropriate icon to change the reporting period from **Day** to **Month** to **Year**.



Stack Chart and Unstack Chart

Display the bar graph with items/users "stacked" on top of each other (Stack) or placed next to each other (Unstack).



Show Chart Legend and Hide Chart Legend

Toggle the explanation of colors used to identify items/users.

Messages Captured by Each Filter

This report tells you the total number of messages identified as spam during a user-specified period of time and how many of those messages were caught by each filter.

To generate a report:

1. Select **Reporting** in the left pane to display the two categories of reports (**User Reports** and **System Reports**) in the right pane.
2. Click **System Reports** to display the different types of system reports available.
3. Click **Spam vs. Non-Spam**.
4. When the Report is displayed, narrow or widen the scope of the report by selecting a **Start Date** and **End Date**.
5. Click **Run Report** to generate the new report.
(Spam is shown in one color and legitimate email in another.)

Once a report is generated, you can change it by selecting the following icons:



Browse button

Specify the email user you want generate a report on.



Roll Up Date and Roll Down Date

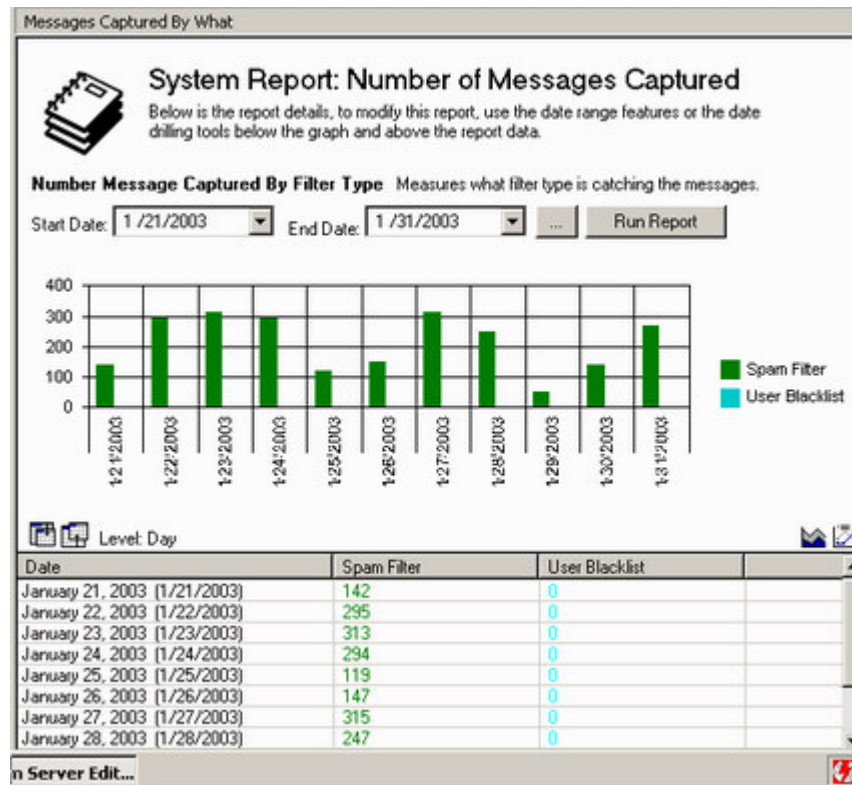
Click the appropriate icon to change the reporting period from **Day** to **Month** to **Year**.

Stack Chart and Unstack Chart

Display the bar graph with items/users "stacked" on top of each other (Stack) or placed next to each other (Unstack).

Show Chart Legend and Hide Chart Legend

Toggle the explanation of colors used to identify items/users.



System Report: Number of Messages Caught by each Filter

Messages Handled by Filtering Engine

The **Messages Handled by the Filtering Engine** report provides an overview of the total email processed by the system (both spam and non-spam) during a user-specified period of time. It also tells you how much spam was caught by each type of filter.

To generate a report:

1. Select **Reporting** in the left pane to display the two categories of reports (**User Reports** and **System Reports**) in the right pane.
2. Click **System Reports** to display the different types of system reports available.
3. Click **Messages Handled by the Filtering Engine**.
4. When the Report is displayed, narrow or widen the scope of the report by selecting a **Start Date** and **End Date**.
5. Click **Run Report** to generate the new report. (Email captured with each type of filter is displayed in a different color.)

Once a report is generated, you can change it by selecting the following icons:



Roll Up Date and Roll Down Date

Click the appropriate icon to change the reporting period from **Day** to **Month** to **Year**.



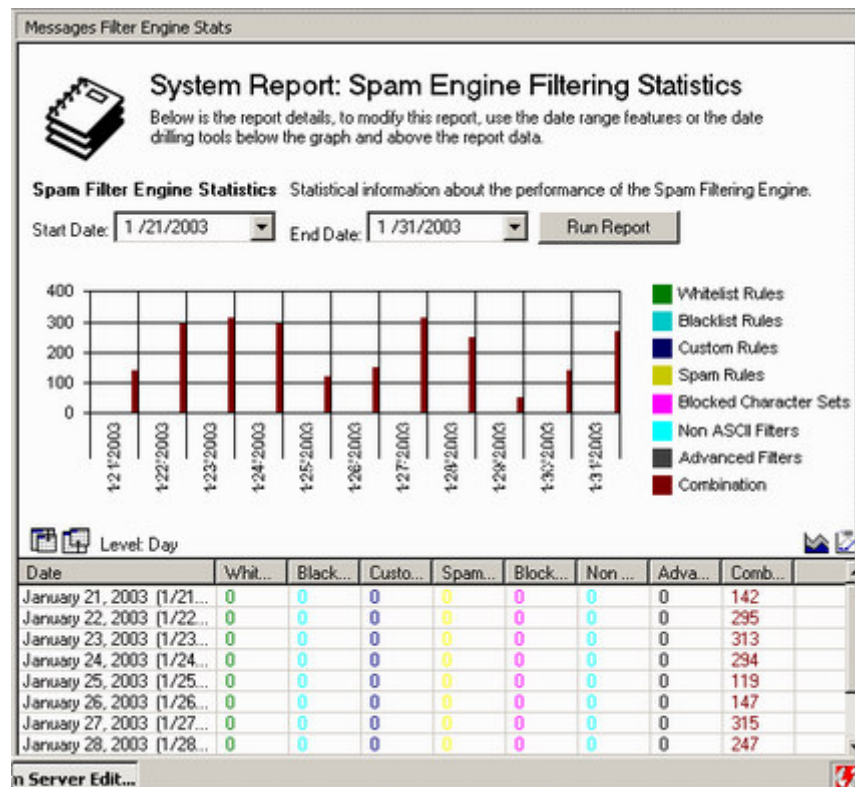
Stack Chart and Unstack Chart

Display the bar graph with items/users "stacked" on top of each other (Stack) or placed next to each other (Unstack).



Show Chart Legend and Hide Chart Legend

Toggle the explanation of colors used to identify items/users.



System Report: Spam Engine Filtering Statistics

Chapter 5: iHateSpam Tools and Support

iHateSpam Server Edition includes the following tools for configuring the system and diagnosing potential problems:

- ❑ Report Database Installation Utility
- ❑ SMTP Events Installation Utility

These utilities can be accessed via the **Tools** menu (**Start/Programs/iHateSpam/Tools**) or from within the **iHateSpam Server Edition Management Console**.

Report Database Installation Utility

iHateSpam Server Edition includes the optional ability to generate extensive reports detailing its filtering of incoming email. The reporting component can be installed during the initial installation of iHateSpam. You can also install it later by running the **Report Database Installation Utility** from the Tools menu (**Start/Programs/iHateSpam/Tools**).

- ❑ If you opt to install the reporting component, you are asked to provide information on how to connect to your database server.
- ❑ After entering the required information, verify that iHateSpam Server Edition can connect to the server by clicking the **Check** button.
- ❑ After verifying your connection, click **Install Reporting**. iHateSpam now creates a new database for reports.
- ❑ After installing the reporting component, you can enable or disable the reporting capability or change your server address or login information from the **Reporting Settings** screen (under System Management).

SMTP Events Installation Utility

iHateSpam Server Edition connects to your **Exchange 2000 SMTP Server Gateway** via **SMTP OnArrival Event Sinks**. The SMTP OnArrival Event Sink must be registered with iHateSpam in order to provide email filtering capabilities to your email users. You must install an SMTP Event Sink on each of your Exchange SMTP services as well as all instances of the services that Exchange uses.

To install SMTP event sinks:

1. Select **SMTP Events Management** (under System Management).
OR
Run the **SMTP Events Installation Utility** from the **Tools** menu by selecting **Programs, iHateSpam, Tools** from the **Start Menu**.
2. If one or more SMTP instances are listed as requiring installation of an Event Sink, place a check in the appropriate checkbox.
If all SMTP instances have Event Sinks installed, existing instances are grayed out and cannot be checked. In addition, a message is displayed indicating that all SMTP Instances have Event Sinks installed.



SMTP Event Sink Installation Dialog

Error Logs

As it performs its job of filtering your incoming email, iHateSpam creates log files that can be useful in resolving technical issues. Logging options are enabled via the **General Settings** screen under **System Management**; the log files are stored in the iHateSpam program directory.

- ❑ Standard **log files** record possible **system errors**.
- ❑ **Trace files** [which have filenames in the format debugGIANT*.log] record **all events** that occur during operation of the system. Trace files are **extremely** large. For this reason, trace mode should **ONLY** be enabled at the direction of support personnel.

Technical Support

If you need additional information about iHateSpam Server Edition, visit Sunbelt Software on the Internet at:

<http://www.sunbelt-software.com/support>

If the answer to your question cannot be found in our Knowledge Base, email our technical support staff:

support@sunbelt-software.com.

Index

- .CSV, 16
- .TXT, 16
- 30-day Demo, 8
- Add Character Set, 12
- Add New Custom Rule, 13
- Block Non-ASCII Email, 12
- Blocked Character Sets, 12
- Character Sets, 12
- Components, 3
- Custom Filtering Rules, 13
- Custom Rules, 13
- Defintions, 11
- Demo Version, 8
- Disable Bounce Message Filtering, 11
- Edit Filter Pipeline, 20
- Email Filtering, 11
- Event Sinks, 9, 28
- Events Management, 9, 28
- Exchange 2000 SMTP Server Gateway, 9, 28
- Export Filters, 16
- Exporting Global Filter Lists, 16
- Features, 3
- Filter Pipeline Overview, 20
- Filter Rules, 13
- Filtering Overview, 11
- Filtering Settings, 11
- Foreign Character Sets, 12
- General Filtering Settings, 11
- iHateSpam SMTP Events Installation Utility, 9, 28
- Licenses, 8
- List Export, 16
- Management Console, 3
- Microsoft Management Console, 3
- Modify Existing Rule, 13
- Operator, 13
- Pipeline, 20
- Property, 13
- Publishing Settings, 10
- Registration, 8
- Registration Key, 8
- Remove Character Set, 12
- Remove Custom Rule, 13
- Replication, 10
- Reports by User, 21
- Rules, 13
- Seats, 8
- Smart Cache, 10
- SMTP Events Management, 9, 28
- SMTP OnArrival Event Sinks, 9, 28
- SMTP Server, 9, 28
- Spam Definitions, 11
- Spam Filtering, 11
- Statistical Reporting, 21
- Statistics, 23
- System Reports Overview, 23
- System Statistics, 23
- Text Format, 16
- Trial Version, 8
- Unicode Text Format, 16
- Update Definitions, 11
- Update Registration, 8
- Update Settings, 10
- User Reports Overview, 21
- Value, 13
- Weights, 13

END USER LICENSE AGREEMENT FOR IHATESPAM SERVER EDITION

SUNBELT SOFTWARE
End User License Agreement
iHateSpam™ Server Edition for Exchange 2000

This Software Product is protected by intellectual property laws and treaties. The Software Product is licensed, not sold.

PLEASE CAREFULLY REVIEW THE FOLLOWING TERMS AND CONDITIONS OF THIS SOFTWARE PRODUCT LICENSE (THE "LICENSE AGREEMENT"). THIS LICENSE IS A LEGALLY BINDING CONTRACT BETWEEN YOU (THE "LICENSEE") AND SUNBELT SOFTWARE PRODUCT DISTRIBUTION, INC. ("SUNBELT").

1. **INTRODUCTION:** The following Software license terms and conditions apply to all of the Software Product (the "Software Product") that is delivered or downloaded under this license. If, after reviewing the terms and conditions which follow this paragraph, you do not wish to be bound by its provisions, do not download the Software Product or, if the Software Product has been delivered by CD ROM, destroy the CD ROM or return it to Sunbelt. If the Software Product has already been downloaded then immediately delete the Software Product. Once the Software Product has been downloaded or accessed all of the provisions of this License Agreement apply, even if the Software Product is subsequently deleted or returned. Any use of the Software Product by the Licensee shall constitute unqualified acceptance of this Agreement.
2. **EVALUATION VERSION LICENSE GRANT:** If you have downloaded or otherwise received an evaluation version of the Software Product, you are authorized to use the Software Product on a royalty-free basis for evaluation purposes only during the initial evaluation period of generally, thirty (30) days. You have the option to register for full use of the Software Product at any time during the evaluation period by following the instructions in the accompanying documentation, including the payment of the required license fee. Registration will authorize you to use an unlocking key which will convert the Software Product to full use, in accordance with the terms and conditions provided below. Your use of the Software Product for any purpose after the expiration of the initial evaluation period is not authorized. Upon expiration of the limited evaluation period, the Software Product may automatically disable itself.
3. **GRANT OF LICENSE.** This Section of the License Agreement describes your general rights to install and use the Software Product. The license rights described in this Section are subject to all other terms and conditions of this License Agreement. Any use, modification, reproduction, release, performance, display or disclosure of the Software Product shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.
 - 3.1. **LICENSE:** The Software Product is provided on a non-exclusive, non-transferable basis, and may not be copied, modified, or enhanced without the advance written authorization of Sunbelt. The Software Product includes significant elements, including its organization, algorithms, and logic, which Sunbelt has maintained as confidential information, which constitute trade secrets of Sunbelt, and which are protected by U.S. patent and/or copyright law and international treaty. Licensee agrees not to attempt to disassemble, reverse compile, or reverse engineer the Software Product. The Software Product under this Agreement is the exclusive property of Sunbelt. This License Agreement does not grant Licensee any ownership right or title to, or interest in the Software Product or any part thereof, and Sunbelt retains all such rights, title, and interest.
 - 3.2. **GENERAL LICENSE GRANT TO INSTALL AND USE THE SOFTWARE PRODUCT.** This license allows you install the Software Product on a server and to only run the Software against the limited number of Exchange 2000 mailboxes that you actually paid a license fee for.
 - 3.3. **RESERVATION OF RIGHTS.** All rights not expressly granted under this License Agreement are reserved by Sunbelt.
4. **DISCLAIMER OF WARRANTY:** THE SOFTWARE PRODUCT IS PROVIDED "AS IS" AND WITHOUT WARRANTY EXCEPT AS PROVIDED IN THE FOLLOWING PARAGRAPH. SUNBELT DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES OF NON-INFRINGEMENT AND PERFORMANCE.

5. **LIMITED WARRANTY:** Sunbelt warrants that the Software Product covered by this License Agreement will, for a period of thirty (30) days following its installation, operate in accordance with the specifications found in the manual accompanying the Software Product.
6. **LIMITATION OF LIABILITY:** Sunbelt makes no representations or warranties that the operation of the Software Product will be uninterrupted or error free, or that it will produce the results desired by the Licensee. Sunbelt does not agree to provide modifications, enhancements, improvements or bug corrections, even if errors in the Software Product are reported to Sunbelt. **SUNBELT SHALL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OR BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, ETC.) ARISING FROM LICENSEE'S USE, OR THE INABILITY OF LICENSEE TO USE, THE SOFTWARE PRODUCT, EVEN IF SUNBELT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**
7. **LICENSEE REMEDY:** If Sunbelt is liable to Licensee for the breach of any of Sunbelt's obligations under this License Agreement, Licensee's sole and exclusive remedy shall be, at Sunbelt's option, to either receive a refund for the price Licensee paid for the use of Sunbelt's Software Product (less any taxes, shipping fees, etc.), or the repair or replacement of any defective Software Product.
8. **LIMITATION ON EXPORTS:** Licensee agrees that Licensee will not export or re-export the Software Product outside of the United States to any individual, business, third party, or other entity, or to any country subject to United States export restrictions, including specifically Iran, Iraq, Cuba, Libya, and North Korea. Any Licensee who receives the Software Product outside the United States agrees not to re-export the Software Product except as permitted by laws of the United States.
9. **U.S. GOVERNMENT RIGHTS:** If you are obtaining Software Product on behalf of any part of the United States Government, the Software Product shall be deemed "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR 12.212, as applicable.
10. **MISCELLANEOUS:** Licensee may make one backup copy for archival purposes only of the Software Product, provided Licensee agrees not to grant access to such backup Software Product to any other individual or business entity. Licensee agrees not to alter or delete any copyright notice which is included with the Software Product. Except as expressly stated herein, there are no other agreements, understandings between the parties, or obligations on the part of Sunbelt relative to the Software Product. The laws of the State of Florida shall apply to the terms of this License Agreement.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND UNDERSTAND IT, AND THAT BY INSTALLING OR USING THE SOFTWARE PRODUCT YOU AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT THIS AGREEMENT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE RIGHTS AND LIABILITIES OF THE PARTIES. THIS AGREEMENT SUPERSEDES ALL PRIOR ORAL AGREEMENTS, PROPOSALS OR UNDERSTANDINGS, AND ANY OTHER COMMUNICATIONS BETWEEN US RELATING TO THE SOFTWARE PRODUCT OR THIS AGREEMENT.